5 Tips for Lifecycle Security for Containers

When you start thinking about full-lifecycle container security, there are a lot of moving parts to keep track of in your pre-runtime and runtime stages. It can be a daunting task—where do you start to look from a best-practices perspective? Here are 5 main areas to consider:

Trust your Registry

› Only allow deployments from trusted and, if possible, internal container registries. Don't allow personnel to pull from unvetted, public images without scanning first.

Implement the Path of Least Privilege

› Whenever possible, only allow non-privileged containers to run that don't have direct access to the underlying host. Basically, give access to only what is required to do the job.

Layered Security is Best

› Combine tactics of pre-runtime container build security with runtime-level container security for total, comprehensive protection.

› Check your images for malware, secrets, and open-source package vulnerabilities while simultaneously providing runtime-level protection at the Kubernetes® cluster level and continuously scanning your registry images for new threats.

Integration is Key for Success

› Foster adoption and champion security best practices throughout your organization by integrating container security with tools you are currently using.

› Vet and scan your images for problems as they are built (if you are using CI/CD practices). It is a lot easier to fix issues during the build process prior to runtime.

› Avoid post-deployment security issues by implementing controls when an image is deployed to your runtime cluster and utilizing tactics, such as admission controls, at the cluster level to guarantee this.

› Ease the burden of deployment by enacting container security with native methods such as helm.

Reduce Your Attack Surface

› Establish a strong foundation by building your application upon scanned, hardened container images, or if possible, try utilizing new distroless container images.

› Using these tactics reduces your attack footprint—especially when you employ new concepts such as distroless images, which slims down the image to only allow the dependencies and packages that application needs to run.

Trend Micro is committed to providing solutions to assist with these efforts. If you are searching for an integrated solution that encompasses these 5 main areas of container security, take a look at Trend Micro Cloud One™ – Container Security. This platform combines 3 main areas such as continuous container image scanning at both the registry and build pipeline, container admission control to your Kubernetes cluster, and runtime level security at the cluster level. Start experiencing container security today with a free trial for Trend Micro Cloud One™.

#TrendTips

TREND MICRO™

[SCS01_Container_Security_210301US]